Different Attacks on Selective Encryption in RSA based Singular Cubic Curve with AVK and Their Possible Solutions

Kalpana Singh[1] and Shefalika Ghosh Samaddar[2]
Corresponding Author & M.Tech IV Semester Student[1], Faculty Member[2]
Department of Computer Science and Engineering
Motilal Nehru National Institute of Technology Allahabad, Uttar Pradesh -211004, India
Email: Kalpana08.mnnit@gmail.com[1], shefalika99@yahoo.com[2]

Abstract- **In this paper, the security of Selective Encryptionin RSA based Singular Cubic Curve with Automatic Variable Key (AVK) for some well known attacks are analysed. It is proved that this cryptosystem is more secure than Koyama scheme from which the algorithm has been generated. The proposed cryptographic algorithm makes justified use of Koyama Schemes. Koyama scheme is not semantically secure. The proposed Scheme is efficient and semantically secure public key cryptosystem based on Singular Cubic Curve with AVK. Further, the partially known attacks, linearly related plain text attacks, isomorphism attacks, low exponent attacks, Wiener's attack and Hastad's attack are analyzed for effect with the proposed scheme. The Selective Encryption in RSA based Singular Cubic Curve with AVK for text based documents is found to be robust enough to encounter all these attacks.**

Keywords- **Singular Cubic Curves, Koyama Public Key Cryptosystem (PKC), Automatic Variable Key (AVK), Semantic Security.**

I. Introduction

Standard RSA public key cryptosystem based on Singular Cubic Curve has given different variants as investigated by different researchers. Three public key cryptosystem were proposed by Koyama. These are called Koyama schemes. The concept of Singular Cubic Curve in Koyama scheme is introduced for the first time to deliver a public key cryptosystem. Singular Cubic Curve is a mathematical tool, which was first time used by Koyama for the construction of public key cryptosystem (PKC). The Singular Cubic Curve is an important concept in number theory because of its wide range of applications. The property of Singular Cubic Curve is helpful in cryptography as it forms an abelian group over finite field. In these schemes two plain texts are (m_x, m_y) are used to form a point $M = (m_x, m_y)$ on the Singular Cubic Curve Curve over Z_n and the cipher text is a point C = em on the same Curve. Singular Cubic Curve over the finite field and the ring F_p is used. Here n is the product of two distinct odd primes greater than 3.

A congruence equation of the form:

$$y^2 + axy = x^3 + bx^2 \mod p \quad (1)$$

where $a, b \in Z_p$ may produce a number of solution. The set of all solutions $(x, y) \in F_p \times F_p$ to (1), is called the solution space of the given singular cubic curve.

Later, Seng et al.[1] have shown that all three Koyama schemes are equivalent to each other by an proposed isomorphism and becomes insecure in the case of some known attacks like partially known attack [2][3], linearly related plain text attack [4][5] isomorphism attack [4], homomorphism attack [6], Wiener's attack [7], and Hastad's attack [7]. Some other security notions are non-malleability [8] and Plain text-Awareness [8]. Non- malleability implies that any attacker cannot modify a cipher text while keeping any control over the relation between the resulting plain text and original one. The Plaintext-Awareness ensures that no one can produce a valid cipher text without knowing the corresponding Plain text. There are a number of mathematically induced attacks on RSA based cryptosystems.

These are classified into three categories:

- Attacks exploiting the polynomial structure of RSA.
- Attacks based on its homomorphism nature.
- Attacks due to a bad choice of parameters employed in RSA.

There are few attacks on RSA which do not require to factor the modulus. Such attacks are sometimes possible when the cipher texts and some additional information are known, for example,

- When some parts of the plain text is also known,
- The encryption of the same or related plain text is sent to different users (e.g. in a broadcast application) or
- When the encryptions of two related plain texts are sent to the same user. This cryptosystem is most commonly used for providing privacy and ensuring authenticity of data.

The efficiency and security [8] are two key factors of any cryptosystem. The cryptosystem proposed by Koyama is not semantically secure [3]. The cipher text should not leave any useful information about the plain text in an ideal situation. The cryptosystem proposed by Koyama is two times faster than that of standard RSA [7] scheme. But it is also not secure against partially known plain text attack, linearly related plain text attack, isomorphism attack, homomorphism attack and These attacks are not possible in Singular Cubic Curve based RSA with AVK technique. This scheme is claimed to be semantically secure and also prevents those attacks which are prevalent in Koyama's scheme. The rest of this paper is organized as follows:

Section 2 presents the related work in this field. Section 3 describes some known attacks and their proposed

DOI: 01.IJIT.01.01.41

solution in an elaborate manner proving the proposed scheme as semantically secure. Section 4 further probes into other kinds of attacks that may happen in such scheme. This section is actually paving the way for future research for finding solution of other attacks. Countermeasures are suggested in Section 5. Efficiency and security analysis of the suggested solutions are the points of concern in Section 6. Section 7 concludes the paper with a future direction of work.

II. Related work

Singular Cubic Curve RSA with Automatic Variant Key (AVK) scheme is based on selective encryption with automatic time variant key (AVK). Selective encryption [9] provides a number of advantages in secured communication process. In the selective encryption, only a random part (*r*) of whole message/plain text is encrypted. Let the selected text be

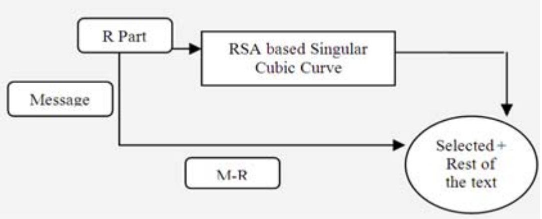

Figure.1: Selective RSA based Singular cubic curve

$R = [r_{ij}]$, where i = bit position row wise, j = bit position column wise. Here $I = 1,2,\ldots\ \ldots n$ and $j = 1,2,\ldots\ \ldots,m$ with i and $i >= 1$, where n and m is linked with the block size and key size respectively$(n \neq m)$ The number of blocks that can be obtained from $[r_{ij}]$, will depend on the family of encryption algorithm. The encryption technique may prevent a key size going beyond a threshold value and such conditional implication can be obtained by right choice of m. If $m = \|[r_{ij}]\|$ then it is one time pad in effect. Rest of the text $= M - [r_{ij}]$is the remaining text after selection. Message$M$ can be presented in matrix format$M = [m_{ij}]$.$R = [r_{ij}]$is a matrix, so$M - [r_{ij}]$is a valid matrix. Therefore, matrix manipulation can be applied for any cryptographic exploitation as as per valid matrix operation. To construct such a scheme, random part of plain text is chosen for encryption/decryption. By applying AVK in this selective text, the desired result is achieved. The key has been automated by design to get changed in every session. The scheme proposed is a generalization of the Koyama scheme. The paper contributes towards the robustness by applying Time Variant key [6] or Automatic Variant Key (AVK) . The concepts of AVK [12][13] is illustrated in [17]. Following basic operations are used in the proposed PKC.

A. Proposed Generalization of Koyama Scheme-II using AVK with application of Selective Encryption

The algorithm demands the implementation of the steps of key generation, encryption and decryption. The steps can be elaborated as follows:

- Select a part $[r_{ij}]$ from M.

Step 1: Key Generation

1) Select large prime number p,qp, q.
2) n=p * q
3) N= 1cm (p-1,q-1)
4) Select integer e.

If gcd (e,N) ==1) where, 1<e<N then generate public key
Calculate: d_p and d_q
Using,

$$d_p = e^{-1} \bmod (p-1) \qquad (2)$$

$$d_q = e^{-1} \bmod (q-1) \qquad (3)$$

The secret key (p, q, d_p, d_q) is generated.

Key generation process allows the sender and receiver to use the key for further communication.

Step 2: Encryption: Plain text (m_x, m_y) and public key (e,n).

$$c = \left(\frac{m_x^3}{m_y^2}\right)^e \bmod n \qquad (4)$$

$$a = \left(\frac{m_x^3 - m_y^2}{m_x m_y}\right) \bmod n \qquad (5)$$

Sender sends (c,a) to the receiver as the cipher text.

Step 3: Decryption: The shadow cipher text (c,a) with secret key (p, q, d_p, d_q) is received by receiver.

$$C_p = c \bmod p \qquad (6)$$

$$m_p = c_p{}^{d_p} \bmod p \qquad (7)$$

$$C_q = c \bmod q \qquad (8)$$

$$m_q = c_q{}^{d_q} \bmod q \qquad (9)$$

Receiver computes, (m_{x_p}, m_{y_p}) and (m_{x_q}, m_{y_q}) using,

$$C_p(a,0),\quad a_p = a \bmod p \qquad (10)$$

$$C_q(a,0),\quad a_q = a \bmod q \qquad (11)$$

Using isomorphic mapping, following can be obtained

$$m_{x_p} = \frac{a_p^2\ m_p}{(m_p - 1)^2} \bmod p \qquad (12)$$

$$m_{y_p} = \frac{a_p^3\ m_p}{(m_p - 1)^3} \bmod p \qquad (13)$$

$$m_{x_q} = \frac{a_q^2\ m_q}{(m_q - 1)^2} \bmod q \qquad (14)$$

$$m_{y_q} = \frac{a_q^3\ m_q}{(m_q - 1)^3} \bmod q \qquad (15)$$

Finally resolving the equations (12)-(15)

$$(m_{x_p}, m_{y_p}) \in C_p(a_p, 0) \qquad (16)$$

$$a_p = a \bmod p \qquad (17)$$

$$(m_{x_q}, m_{y_q}) \in C_q(a_q, 0) \qquad (18)$$

$$a_q = a \bmod q \qquad (19)$$

By application of Chinese Remainder Theorem [14] on following equations:

$$(m_{x_p}, m_{y_p}) \in C_p(a_p, 0) \qquad (20)$$

$$(m_{x_q}, m_{y_q}) \in C_q(a_q, 0) \qquad (21)$$

DOI: 01.IJIT.01.01.41

Resolving $(m_x, m_y) \in (a, 0)$.

Encryption has been applied on selected part of the text message M only and therefore named as selective encryption technique. Decryption has been applied on selected part using the similar algorithm by the receiver. Finally, the full text document can be constructed by merging the decrypted selected part of M namely $[r_{ij}]$

with the remaining part of the message.

Thus

$$[r_{ij}] + (M - [r_{ij}]) = M \qquad (22)$$

Can be obtained.

III. SOME KNOWN ATTACKS AND THEIR PROPOSED SOLUTIONS

A.. Partially known plain text attack and its solution:

In the Koyama scheme, knowing one ordinate m_X or m_Y in a plain text pair(m_x, m_y)one can compute the whole plain text with the help of corresponding cipher text. Let n, e be a public key and $C = (c_x, c_y)$be the encryption of the plain text $M = (m_x, m_y)$, i.e. $e \otimes (m_x, m_y) = (c_x, c_y)$Assume that m_x is known and m_y is unknown. Let $m_y = y$. Then, $e \otimes M$ over $\frac{Z[y]}{(y^2 - m_x^3 - bm_{x,}, n)}$by using the addition law of *Singular* Cubic Curve. For the Koyama scheme, by induction technique, it can be shown that for any k in Z_n, $k \otimes (m_x, y) \equiv (u_k, v_k y)$ where u_k and v_k are two positive integers. Finally, for $k = e$, the relation $(u_e, v_e y) = (c_x, c_y)$, which can be solved for $y = c_y v_e^{-1} (mod\, n)$ if $ve \neq 0\ (mod\, n)$. However, if $v_e = 0\ (mod\, n)$ then the cipher text C is a point of order 2 in $C_n(0, b)$ which means that $d \otimes C = M$, i.e. $C = M$, hence M is always computable. *In case of Selective Encryption in Cubic Curve RSA with AVK:* Let the selected part of document be equal to complete part.

$(u_e, v_e y) = (c_x, c_y)$, Comparing both sides $v_e y = c_y$ =>

$$y = c_y v_e^{-1}\ (mod\, n)$$

if v_e 0 ($mod\, n$), and if is known, (c_x, c_y) = c, d—" c = M (original plain text) If attacker hacks this data, and wants to decrypt the data due to AVK, the attacker can not find the decrypted key applied over the text iteratively even if he/she is successful in getting hold of immediate key that gets changed in the next iteration, Hence this attack cannot be successful.

B. Security against Linearly related plain text attack:

Koyama scheme is insecure if two linearly related plain texts are encrypted with same public key. This attack is explained as follows: Let M =(m_x, m_y) and M'= (m'_x, m'_y) be two plain texts linearly related by the known relations:

(m'_x, m'_y)be two plain texts linearly related by the known relations :

$$m'_x \equiv \alpha m_x + \gamma \qquad (23)$$
$$m'y \equiv \beta m_x + \delta \qquad (24)$$

where α, β γ and δ are integers in Z_n^*. Assume that the encryption of the plain texts $(m_x, m_y)$and (m'_x, m'_y) are given by:

$$(c_x, c_v) \equiv e \otimes (m_x, m_v)\ (mod\, n) \qquad (25)$$
$$(c'_x, c'_v) \equiv e \otimes (c_x, c_v)\ (mod\, n) \qquad (26)$$

From the above cipher text it can be derived the curves $C_n(0, b)$ and $C'_n(0, b\ )$ upon which the point must lie. Thus it is derived.

$$m_x^3 + bm_x^2 - m_v^2 \equiv 0\ (mod\, n) \qquad (27)$$

$$(\alpha m_x + \gamma)^3 + b'(\alpha m_x + \gamma)^2 - (\beta m_v + \gamma)^2 \equiv (mod\, n) \qquad (28)$$

from last two equations m_v can be derived as a polynomial w in m_x with $w(x) = (\alpha m_x + \gamma)^3 + b'(\alpha m_x + \gamma)^2 \beta^2 \frac{(\beta m_y + \gamma)}{2\beta\alpha}$

(29)

By using the addition formula on Singular Cubic Curve, it is clear that $w(m_x) \equiv m_y (mod\, n)$. Now let $f(x) \equiv x^3 + bx^2 - w(x)^2 (mod\, n)$

(30)

which is a polynomial of degree 6. Thus

$$f(m_x) \equiv 0 (mod\, n) \text{ on } Z_x/(n, f_x) \qquad (31)$$

Next, $e \otimes (x, w(x)) \equiv (h(x), j(x)) (mod\, n)$ is computed over $Z[x]$ /$(n, f\ (x))$. Then the following equations are obtained:

$$h(m_x) \equiv c_x (mod\, n) \qquad (32)$$
$$j(m_x) \equiv c_v (mod\, n) \qquad (32)$$

Finally, $gcd(h(x) - cx, f\ (x))$ is computed which is a linear Singular polynomial of the form $k(x - mx)$. This gives the plain text text based m_x. After knowing the half of the plain text (m_x, m_y) = M , the other half $m_y$can be computed by $w(m_x) = m_y$. Again by the linear relation between M and M', the plain text M' can be computed. In order to apply such type of attack, the knowledge of parameter b (or a)is necessary.

Selective Encryption in Singular Cubic Curve RSA with AVK:

The relationship does not hold good and therefore decryption or finding the key at a particular stage (though being linearly dependent texts) is not possible as the iterative stages may not be the same due to different plaintext.

C. Security Security against Isomorphic attack

The idea behind this type of attack is based on the isomorphic property of two Singular Cubic Curves. Such type of attack was first time identified by Koyama for the KMOV scheme [6]. The isomorphic property may be described by using the following theorem.

Theorem: *Let* $n = pq$ (p, q are primes), and $c_n(0.b_1)$and $c_n(0.b_2)$be Singular Cubic Curves such that,

$c_n(0.b_2)$be Singular Cubic Curves such that,

$$C_n(0,\ b_1): y^2 = x^3 + b_1 x^2 (\text{mod } n), \qquad (34)$$
$$C_n(0,\ b_2): y^2 = x^3 + b_2 x^2 (\text{mod } n). \qquad (35)$$

$C_n(0,\ b_1)$ and $C_n(0,\ b_2)$ are isomorphic if there exist $u_p \in Z_p^*$and $u_q \in Z_q^*$such that,

$$b_2 \equiv u_p^2 b_1 (\text{mod } p), \qquad \text{and} \qquad b_2 \equiv u_q^2 b_1 (\text{mod } q)$$

By using the property of Singular elliptic curve over field and Chinese Remainder Theorem, the following isomorphic property of Singular Cubic Curve over ring is shown [15] as follows:

DOI: 01.IJIT.01.01.41

$C_n(0, b_1) : y^2 = x^3+b_1x^2 (\text{mod } n)$ (36)

and $C_n(0, b_2): y^2 = x^3+b_2x^2(\text{mod } n)$ (37)

Let $M_1 = (m_{1x}, m_{1y})$, $C_1 = (c_{1x}, c_{1y}) \in C_n(0, b_1)$ and $M_2 = (m_{2x}, m_{2y})$, $C_2 = (c_{2x}, c_{2y}) \in C_n(0, b_2)$, where $C_1 = e \otimes M_1$ over $C_n(0, b_1)$ and $C_2 = e \otimes M_2$ over $C_n(0, b_2)$.

Then the following statements are considered equivalent,

i. $C_n(0, b_1)$ and $C_n(0, b_2)$ are isomorphic

ii. $b_2 \equiv u^2 b_1 (\text{mod } n)$ for some $u \in Z_n^*$

iii. $c_{2x} \equiv u^2 c_{1x} (\text{mod } n)$, $c_{2y} \equiv u^3 c_{1y} (\text{mod } n)$ for some $u \in Z_n^*$

iv. $m_{2x} \equiv u^2 m_{1x} (\text{mod } n)$, $m_{2y} \equiv u^3 m_{1y} (\text{mod } n)$ for some $u \in Z_n^*$

If C_1, C_2 and M_1 satisfying the congruence (3) are given, then M_2 can be easily obtained by computing the congruence (4). It is not difficult to check whether congruence (2) holds. Suppose, an attacker A wants to victimize B by forging signature on a plain text $M = (m_x, m_y)$ without B's consent. For this, A generates another message M' with B's public key n_B and random integer u:

$M' = (u^2 m_x \text{mod } n_B, u^3 m_y \text{mod } n_B)$,

and sends M' to B. B makes a signature $S' = (s_x', s_y')$ for M' with his secret key d_B:

$$S' = d_B \otimes M' \text{ over } C_{nB}(0, b_B').$$

Then, A computes the signature.

$S = (s_x, s_y) = (u^{-2} s_x' \text{mod } n_B, u^{-3} s_y' \text{ mod } n_B)$. (38)

Which is B's signature for the message M. It may be noted that the curve $C_{nB}(0, b_B)$ contains points (M, S) and the curve $C_{nB}(0, b'_B)$ contains points (M', S'). Using this technique, A can forge B's signatures without B's secret key.

Selective Encryption in Singular Cubic Curve RSA with AVK:

allows M' to be sent to receiver B. B makes a signature $S = (s_x, s_y)$ for M' with his secret key d_B This d_B is not original d_B, in which AVK function has been applied and the function is represented as AVK (d_B).B will calculate the signature as follows:

$S = AVK\ (d_B). M \text{ over } C_n\ (0, b_B)$ (39)

The attacker can not find the secret key of B in this computation. Hence Isomorphic attack is not possible in case of selective encryption with AVK.

D. Security Security against Homorphic attack

This attack originated from homomorphic propert (k⊗[P + Q] = k⊗[P] ⊕ k⊗[Q]), Some known attacks of this typ come under homomorphic attacks. Using homomorphic property such as common modulus attack, chosen message attack, garbage man-in-the-middle attack, the Koyama schemes

E. Common Modulo attack

If a message M is sent to two users who have co-prime public encryption keys (say e_1 and e_2), then the message M can be recovered by way of computation. Let the cipher text corresponding to the plain text M are $C_1 = M^{e_1}\ (\text{mod } n)$ and $C_2 = M^{e_2}\ (\text{mod } n)$a, then by extended Euclidean algorithm, attacker C can compute u and v such that $ue_1 + ve_2 = 1$, and he can easily get the plain text M by computing $C_1^u C_2^v n = M$, $e_1 u + e_2 v\ (\text{mpd } n) = M$ This attack is called common modlus attack.

[Input] Two cipher texts$C_1 = (C_{x_1}, C_{y_1})$,$C_2 = (C_{x_2}, C_{y_2})$common modulus n, and encryption keys e_1, e_2.

[Step1] By extended Euclidean algorithm Carol computes u and v such that $e_1 u + e_2 v = 1$

[Step2] Attacker C computes,

$$u \otimes (c_{x_1}, c_{y_1}) \oplus v \otimes (c_{x_2}, c_{y_2})$$

$$= (u \times e_1 + v \times e_2) \otimes (m_x, m_y)$$

$$= (m_x, m_y)$$

[Output] The intended plaintext pair (m_x, m_y).

In Selective Encryption in Singular Cubic Curve RSA with AVK, AVK function has been applied after encryption. So,

$$u \times (C_{x_1}, C_{y_1}) + v \times (C_{x_2}, C_{y_2})$$
$$= (u \times AVK(e_1 + v \times AVK(e_2))$$

it cannot be found out e_1, $e_2$from the equation without having further information on e_1, and e_2 Hence, this attack is not possible if this algorithm is used for cryptography.

F. Chosen Message attack

Chosen Message Attack is possible in Koyama schemes Suppose an attacker C wants to get the signature of a sender A on the message pair (m_x, m_y) Then he proceeds as follows:

[Input] A message pair (m_x, m_y) and the key n, e of plaintext.

[Step1] First Carol chooses relatively prime to and computes and such that ev + ku = 1.

[Step2] Carol computes $M' = k \otimes (m_x, m_y) = (m'_x, m'_y)$.

[Step3] Next, she ask Alice to sign on the document $M' = (m'_x, m'_y)$ and gets the signature $S' = d \otimes (m'_x, m'_y) = (s'_x, s'_y)$.

[Step4] Consequently Carol can compute the signature S of M by,

$$S = \{u \otimes (s'_x, s'_y)\} \oplus \{v \otimes (m_x, m_y)\}$$
$$= \{(u \times d \times k) \otimes (m_x, m_y)\} \oplus \{v \otimes (m_x, m_y)\}$$
$$= d \times (uk+ev) \otimes (m_x, m_y)$$
$$= (s_x, s_y)$$

[Output] The signature S of M.

In Singular Cubic Curve RSA with AVK, when attacker sends

Message (m'_x, m'_y) to the sender for knowing the secret key,

the attacker gets the signature $S' = d \times (m'_x, m'_y) = (s'_x, s'_y)$.

After signing by the sender, then sender will apply the function of AVK as follows:

$S' = AVK\left(d \times (m'_x, m'_y)\right)$ (40)

So, attacker can not compute the signature as the function AVK is not giving predictable output in a single step.

DOI: 01.IJIT.01.01.41

$s = u \times (s'_x, s'_y) + v \times (m_x, m_y) = u \times k \times AVK(d \times (m_x, m_y)) + v \times (m_x, m_y)$ AVK function has been applied therefore the equation $((uk + ev) = 1)$ fails to yield the desired output and (sx, sy) could not be obtained. Thus this type of attack is not possible if the proposed algorithm is applied [17].

G. Garbage Man-in-the-middle attack attack

This attack is possible in Koyama scheme. The attacker wants to get the plain text M from a given cipher text C = (c_x, c_v) in the Koyama scheme. The attacker can get original plain text as follows:

[Input] A message pair(c_x, c_y), n , e.

[Step1] First Carol inspects C = e⊗(m_x, m_y) = (c_x, c_y).

[Step2] C'= (c'_x, c'_y) = k⊗(c_x, c_y) = k×e⊗(m_x, m_y) for any chosen k relatively prime to e.

[Step3] By Extended Euclidean Algorithm, Attacker C can compute u, v $\in Z_n$ such that ku+ ev = 1.

[Step4] She ask Alice to sign on (c'_x, c'_y) and gets

S'=(s'_x, s'_y)=d⊗(c'_x, c'_y) = d×k×e⊗(m_x, m_y) = k⊗(m_x, m_y)

[Step5]Now, Attacker C can compute the original Message as,

u⊗(s'_x, s'_y)⊕v⊗(c_x, c_y) = u×k⊗(m_x, m_y) ⊕ e×v⊗(m_x, m_y) = (m_x, m_y).

[Output] The intended plaintext (m_x, m_y).

But in Singular Cubic Curve RSA with AVK, at the time of signature, $S' = (s'_x, s'_y) = d \times (c'_x, c'_y) = d \times k \times AVK(e \times (m_x, m_y))$. Then, attacker can compute the original message as

$$u \times (s'_x, s'_y) + v \times (c_x, c_y) = d \times (c'_x, c'_y) + v \times (c_x, c_y)$$
$$= d \times k \times AVK(e \times (m_x, m_y)) + v \times (c_x, c_y)$$
$$= u \times k \times AVK(m_x, m_y) + e \times v \times (m - x, m_y)$$

By this equation, it is clear that plain text can not be identified as it is the functional output of AVK. Output is not confined in a stepwise manner and very much dependent on data and, therefore the attack is ineffective in the proposed algorithm of proposed approach in this paper.

IV. SOME OTHER KNOWN ATTACKS

A. Wiener's attack

To reduce decryption time, one may wish to use a small value of d rather than a random d. Since modular exponentiation takes time linear in $\log_2 d$, a small d can improve time reduction or increase in speed to a great extent. Wiener[7] shows that a small d results in a total break of the cryptosystem. General description of Wiener's attack as follows:

Theorem: Let N =pq with $q < p < 2q$. Let d<$1/3N^{\frac{1}{4}}$.

Given N,e with ed=1 mod$\emptyset(N)$,Marvin can efficiently recover d.

This can be proved as: Since ed=1 mod$\emptyset(N)$,, there exists a k such that ed-k$\emptyset(N) = 1$. Therefore,

$$\left|\frac{e}{\emptyset(N)} - \frac{k}{d}\right| = \frac{1}{d\emptyset(n)} \qquad (41)$$

Hence: $\left|\frac{e}{N} - \frac{k}{d}\right| \leq \frac{1}{d^{\frac{1}{4}}} < \frac{1}{2d^2}$

This is a classic approximation relation. The number of fraction $\frac{k}{d}$ with d<N approximation $\frac{e}{N}$ so closely is bounded by $\log_2 n$. Since ed-k$\emptyset(N)$=1, therefore, gcd(k,d=1), and hence $\frac{k}{d}$ is a reduced fraction. This is a linear time algorithm for recovering the secret key d. But in linear time algorithm for recovering the secret key d. But in case of singular cubic curve RSA, the concept of AVK has been applied. At receiver side following holds good:

$$d_p = e^{-1} mod(p-1) \qquad (42)$$
$$d_q = e^{-1} mod(q-1) \qquad (43)$$

Before decryption, AVK is required to be applied again and, calculation of AVK is not possible for attacker due to change of key in every session. So this attack is totally avoided in this proposed extension of Koyama scheme [17].

B. Hastad's attack

The Koyama scheme is very much vulnerable to Hastad's attack. Let, Koyama's Singular Cubic Curve equation be:

$$y^2 + ax \equiv x^3 (mod\ n)$$

where the plain text is a pair $(m_x, m_y)$and a is chosen such that the equation with $x = m_x$ and $y = m_y$ is satisfied. An attack is possible when one half of the plain text can be found when the other half is known [16]. From equation plain text can also be recovered when at most 1/6 of m_x andm_y is unknown. When 6 linearly related messages are known then a Hastad attack is possible making Koyama Scheme vulnerable enough.

But in case Singular Cubic Curve RSA with AVK, the linear relation between the consecutive plaintext and cipher text is not established due to change of key in every session, Moreover, the unencrypted plaintext and selectively encrypted cipher text are combined together making it impossible to detect the linearity between the said texts of the document chosen.

DOI: 01.IJIT.01.01.41

V. COUNTER MEASURES AND DISCUSSION ON THEORETICAL SIMULATION

Randomized key concept is applied in AVK in plain text after encryption and at the time before decryption by the receivers should not be chosen too small, since a small would give yet other small modular equations over the plain text that can be combined with $m_x^3 + b \equiv m_y^2 \ (mod\ n)$ for even more effective attacks. Since the degree of the equations resulting from division polynomials is e_2 it is suggested to choose *e* at least 16 bits long. These propositions require, a careful analysis in a case to case basis depending upon the Cipher Suite's requirement.

VI. EFFICIENCY AND SECURITY ANALYSIS

In the scheme given by Koyama, eth power of m_x^3/m_y^2 under modulo n is computed during the encryption process. In case of proposed extension of Koyama scheme as presented by Singh and Samaddar [17] algorithm, selective encryption has been applied, then AVK has been used for security purpose. This feature increases the efficiency of encryption. But, the decryption is approximately of similar efficiency of the schemes given by Koyama.

From Koyama's analysis, let *x* and *y* the coordinates of 2 log *n*-bit plain text be transformed to a log *n*-bit plain text by isomorphic mapping. This message of log *n* bit length is then encrypted by using encryption process. The obtained cipher text is decrypted by using decryption key over which is *n* the transformed message. By using the inverse transformation, the origional 2 log *n* bit length message is obtained. But from the analysis of Koyama schemes, a number of attacks are permissible like Partial known plain text, Linear related plain text attack, Isomorphic attack, Homomorphic attack (Common modulo attack, common modulo attack, Garbage Man-in-the - middle attack), Wiener's attack and Hastad's attack. This proves that Koyama scheme is not semantically secure enough and therefore require enhancement in terms of robustness that has been pointed out here by the introduction of AVK. In case of Selective encryption Singular Cubic Curve RSA with AVK, these attacks are not possible. This algorithm is also proved to be semantically secure due to use of AVK concepts. The proposed system has already been substantiated [17]. The results obtained in this paper on the basis of theoretical simulation and analysis can be substantiated further by computational simulation. This has been taken up for application oriented study in future course of research. Due the page limitation the concerned graph of simulation results could not be produced here that echo the theoretical implications obtained in this paper.

VII. CONCLUSION AND FUTURE WORK TO BE UNDERTAKEN

The robustness of the algorithm [17] over the extension of Koyama Scheme with selective encryption in RSA Singular Cubic Curve with AVK is considered here. The algorithm proposed by Singh and Samaddar [17] is investigated from different angles to come to the conclusion that a number of known attacks are not possible due to the design of the algorithm. Application oriented simulation may be taken up to establish the results beyond any doubt. A future direction of work in this area is to develop a generic algorithm which will be equally applicable to text based as well as image based documents.

References

[1] Seng Kiat Chua , Ka Hin Leung, San Ling, *"Attack on RSA typecryptosystem based on Singular Cubic Curve over cryptosystem based on Singular Cubic Curve over science, Z/ nZ**Theoretical Computer science, Vol.220 19-27 (1999).

[2] Sahadeo Padhye, *"Partial Known Plaintext Attack on Koyama Scheme,"* Information Processing Letters, Vol.96 No.3 pp. 96-100 (2005).

[3] Sahadeo Padhye and B. K. Sharma, *"A Fast Semantically Secure Publication Key Cryptosystem Based on Factoring,"* International Journal of Network Security, Vol.3, No.2, PP.144150, Sept, (2006), retrieved

[4] Sahadeo Padhye, *"Cryptanalysis of Koyama Scheme,"* International Journal of Network Security, Vol.2, No.1, pp. 73-80, (2006).

[5] D. Blichenbacher, *"On the security of KMOV public key cryptosystem,"* Crypto'97 LNCS Springer- Verlag Vol.1294, 235-348, (1997).

[6] Marc Joye and Jean- Jacques Quisquater, "*Cryptanalysis of RSA-Type Cryptosystem: A Visit,*" American Mathematical Society, vol. 38, pp. 21- 31, (1998).

[7] Dan Boneh, " *Twenty Years of Attacks on the RSA Cryptosystem,*" American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203-213, (1999).

[8] Sahadeo Padhye, "*A public key cryptosystem based on singular cubic curve"*, Eprint Archive-2005/109, http: //eprint.iacr.org/ 2005/109.pdf, 2002.

[9] Prof C T Bhunia, Gourchari Mondal and S Samaddar, "*Theory and application of time variant key in RSA and that with selective encryption in AES* ", 2006.

[10] D. Galindo, S. Mortin, J. L. Villar, "*An efficient semantically secure elliptic curve cryptosystem based on KMOV scheme"*, Eprint Archiecve2002.1037/ http//erpint.iacr.org/2002/1037, 2002.

[11] C.T.Bhunia "*Application of avk and selective encryption in improving performance of quantum cryptography and networks,*" United Nations Educational Scientific and Cultural Organization and International Atomic Energy Agency, (2006), retrieved 10/ 12/2009, from http://users.ictp.it/ pub off/preprints-sources/2006/ IC2006045P.pdf.

[12] P. Chakrabarti, B Bhuyan, A.Chowdhuri C.T.Bhunia, "*A novel approach towards realizing optimum data transfer and automatic variable key (AVK)"* IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008.

[13] Deepak Garg, Seema Verma, "*Improvement over public key cryptographic algorithm"*, IEEE, International Advance Computing Conference (IACC), 2009.

[14] Koyama K, "*Fast RSA -type schemes based on Singular Cubic Curves +axy,*" Proceeding in LNCS EUROCYPT 95,Volume - 921 , PP. 329-340.Springer Verlag (1995).

[15] Don Coppersmith, Matthew Franklin, Jacques Patarin, Michael Reitert, "*Low-Exponent RSA with Related Messages,*" Advances in Cryptology - EUROCRYPT '96, LNCS 1070, pp. 1-9, (1996).

[16] Singh, Kalpana and Samaddar, Shefalika Ghosh "*Selective Encryption Technique in RSA based Singular Cubic Curve with AVK for Text Based Documents: Enhancement of Koyama Approach,*" 2010 International Conference on Networking and Information Technology (ICNIT 2010) Manila, Philippines, June 11 - 12, 2010.

DOI: 01.IJIT.01.01.41